Mechatronic Security and Robot Authentication

Wael Adi
Technical University of Braunschweig
Braunschweig, Germany
wadi@ieee.org

***Abstract*—Robot Security is becoming more and more a serious issue for many modern applications. Robot Security matters are still not intensively addressed in the published literature. The goal of this paper is to explore possible identification and security mechanisms which fit to robot technologies and their operating environment. To secure transactions between robots deployed in open service, robots need first to be securely identified "as persons" with unique provable identities. Robots rolling from a production line are assumed to be equal objects; therefore the first necessary action is to personalize robots and give them unclonable identities. A sort of "Electronic mutation" technology was specified and proposed to create a non-reversible and non-repeatable robot identity, which is at the same time securely provable [6]. The identity exhibits properties similar to those of human DNA. The resulting clone-resistant or (unclonable) identity is adapted and proposed to be embedded in a robot environment. The goal is also to diffuse the identity traces possibly into all robot activities similarly as the human DNA do throughout the whole body of a biological creature. The identity proposed is made traceable through cryptographic signatures linked to relevant robot mechanical and electronic activities as a step towards "mechatronic security". The work is also aiming to stimulate discussions on robot security issues or in general the question of "mechatronic security".**

***Index Terms*—Robot Security, Identification Protocols, clone-resistant physical entities , Mechatronic Security**

I. Introduction

THE growing deployment of robots for many security relevant applications is demanding more and more security profiles for robots to deal with individual persons having own unclonable identity. Deploying robots for tasks to replace human beings raises the question of robot authentication approaching a level of confidence similar to that of the human DNA with its particular property of being diffused and spread into the whole human body. Robot identity as a security issue is still not intensively addressed in the published literature. This paper is discussing basic security requirements on robots for security relevant tasks and proposing initial electronic identity setup required to establish later robust secured transactions with robots in their operation environment.

II. Robot as Living Individuals

Setting a strong requirement that the deployed robot should be uniquely identified and authenticated as human beings, leads to a first simple idea to consider a robot as a living creature, which is born at some time point having a non-clonable DNA and which goes through a variety of usual procedures as assigning a name for it and becoming accepted by the community with a confident birth certificate. A robot starts then usual transactions with its environment including learning, developing of its knowledge and capabilities, as well as other living processes such as becoming sick/defect and being treated/repaired and probably having health and disease records. Robots could acquire certified knowledge or skills or have aging and finally after some time a robot may die. Throughout the whole life cycle, the robot should represent a unique individual personality and develops its own personal profile. Considering the robot as creature similar to biological creatures, leads to the idea of inspiring identification mechanisms with different and scalable degree of confidence with multiple attributes even linked to the history and personal profile similar in nature to those of the biological systems.

III. Unclonable and Clone-Resistant Identity

Identifying physical entities or electronic devices in a large system is becoming day by day an essential requirement for building robust and stable secured system. For maintenance and cost reduction reasons, systems are mostly produced by having off-shelf equal electronic devices/chips to be later personalized (as in Smartcards) in initial assembly or setup phase by inserting/programming certain unique bit-stream for later identification during operation in the real field.

Physical Unclonable Functions (PUF) has been introduced making use of some inherent physical differences between devices to uniquely identify electronic devices [1]–[3]. The devices identified by such technique are expected to be perfectly unclonable as the existing large mappings (PUFs)

978-0-7695-3754-2/09 $25.00 © 2009 IEEE
DOI 10.1109/BLISS.2009.30

are not practically reproducible even by the same manufacturer. However, the costly sensing and/or the inherent liability of electronic devices to be sensitive to temperature and voltage drifts make PUF's technique often not adequate for many practical applications. PUF's are permanent and supposed to be time invariant mappings, however their structure in prone to ageing effects which could dramatically limit its lifetime. Therefore, a constructive and consistent identity generation is also considered with a lifetime corresponding to that of the deployed electronic units in the robot. A constructive identity as the proposed one in this paper is considered as a "clone-resistant" identity as it is not intrinsic and can not be considered as a perfect one; however it is more flexible for operational security tasks and allows evolutionary security procedures.

IV. Requirements for Secured Robot Identity

Considering robots for replacing human being in sensitive tasks, the proposed technology should attempt to inspire new electronic identification mechanisms from the real life systems. In such systems, a diversity of identification strategies is deployed to end up with adequate and operational identification in the target robot environment. The following security requirements are to be considered for designing robot identification technology:

1. The robot identity should be *unique and provable*
2. Generating the same identity (cloning) should be technically impossible without great invasive attack. Even then the system should detect successful cloning attacks and resolve it. In other words the system security should be *stable*, *robust and resilient*.
3. Authenticity proof linked to robot identity should diffuse in each robot action when required.
4. Proof of identity should be *scalable* in a sense that many identification certainty levels and varieties can be deployed on demand similar to identifying persons in a living society.
5. The identity should exhibit and develop time variant components and evolutionary aspects as those of persons in real social environment.
6. Trust and identification proofs should allow building chains of *testimony* in a sense that if A trusts B and B trusts C then B can mediate a trust between A and C.
7. Identity based threshold *secret sharing schemes* using robot identity should be realizable.
8. Other scenarios similar to those of the human society can be implemented based on the robot identity

The security requirements catalog can be extended and reduced depending on the robot nature and its operation environment. Some applications may require dropping the majority of authentication profile as anonymous operating environment is needed, other operation environment may required much more identity confidence and more resilient security requirements.

V. Bio-Inspired Robot Identity

A Concept for DNA-like Electronic Identity

In biology, mutations are changes to the nucleotide sequence of the genetic material of an organism. Mutations can be caused by copying errors in the genetic material during cell division, by exposure to ultraviolet or ionizing radiation, chemical mutagens, or viruses, or can occur deliberately under cellular control during processes such as hyper-mutation.

The biological Mutation, if succeeded, is a permanent irremovable change in the genetic properties which *reflects its effects on future* behavior and properties [4].

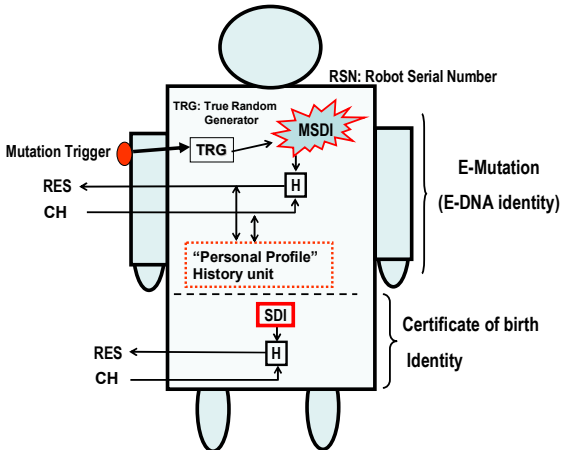

Figure 1. Robot e-Mutation and birth certificate

A basic structural "electronic mutation" e-mutation scenario was introduced in [5]. A sample implementation was demonstrated by deploying a true random generator TRG structure injecting a permanent random value in a register after a "mutation trigger" is activated as shown in Fig.1. The resulting self defined *unknown* identity MSDI (Mutated Secret Device Identity) together with a (possibly even *unknown)* hash function H should be provable but not clonable. The resulting "Mutated Identity" exhibits DNA-like properties as it is provable through challenge response traces of a hidden secret identity without the necessity to be revealed to anybody. This e-mutation can serve to generate a sort of electronic DNA (e-DNA) chain for a particular

device. In other words, fabricating the same devices by the manufacturer can be seen as a mass-cloning operation, the e-mutation is seen as deliberate randomized mutation giving each device its individual e-DNA identity at some time point after production.

The basic identification challenge-response technique deployed is not new as it is widely deployed as a identification protocol successfully practice [3]. The same technique is also deployed for PUF identification mechanisms [1-3]. Referring to Fig. 1, the proposed technique differs from the conventional techniques in that

1. It is merging two major classes of identification technologies, namely the mutated secret "MSDI" and the authority certified identity "SDI".
2. It is integrating and linking the dynamic robot "personal profile: PP" with the above identities to come up with a clone-resistant authentication protocols. A sample cryptological authentication scenario linking all the listed robot entities MSDI, SDI and PP is demonstrated in section 4.
3.

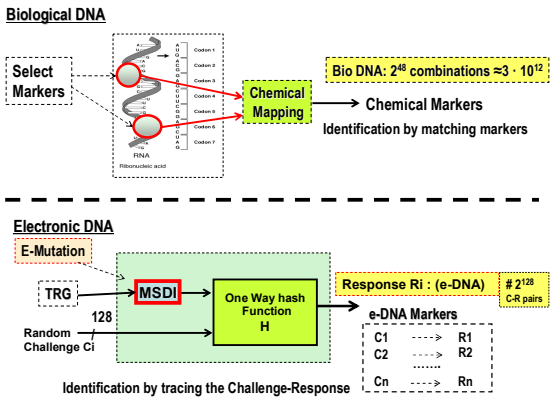

Figure 2. e-Mutation: Biological DNA vrs e-DNA

Fig. 2 shows a simplified, well known identification scenario for physical objects after being challenged once without the need to know the secret mutated identity MSDI and even the function H. The initially generated and secretly kept **challenge-response trace (pairs)** can be used in a later time point to check if the same device is behind the proof response [1]. The cryptological relevance of that trace "marker in medical terminology", is that it is selected from a space having a large size say 2^{128} mapped through unknown function H. Such traces correspond to the DNA markers selected in practical forensic biological identification techniques [4].

Having integrated and linked such properties, cloning a device would become practically equivalent to the difficulty of first cracking the mutated identity with its function H by some invasive attack and then seeking and copying all relevant robot transactions history (possibly unknown). This is near to be impossible in most practical application. Even if a successful cloning was possible, the system would detect discrepancy after some time, as both cloned and non-cloned units would exhibit different evolved identity properties for the same claimed unique name or serial number. This is demonstrated in Fig. 3. Suppose that the units G was successfully cloned at some time and two G units were created having exactly the same properties at the cloning time point. At most, after the first transaction with the system, each unit G would autonomously, (as operationally enforced) generate together with the system new traces/properties caused by two independent processes which are most likely different. The result is two differently-traced objects G' and G'' with different identities toward the system and both of them are claiming to be the object G. The identification process for one of them would certainly fail and both objects are detected. Fraud can first be stopped and further investigations would clear the case and abandon the illegal object.

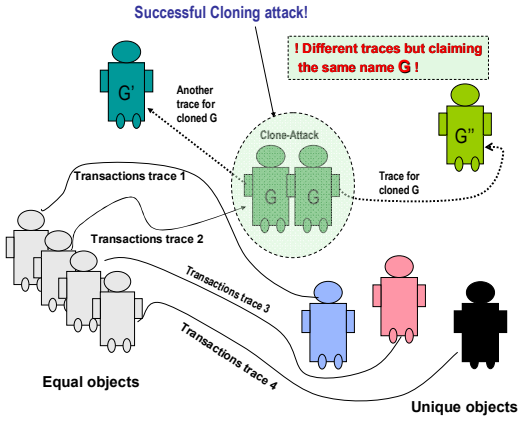

Figure 3. Traced-history and resolving cloning attack

Such detection capabilities are missing in the majority of systems where physical replacement attacks are possible.

VI. Clone-Resistant Robot Identification Scenario

In this section a possible clone-resistant identification protocol linking the secret mutated identity MSID, SDI and unit/robot personal profile in a sample identification scenario. It is demonstrating a possible strong clone-resistant physical robot identity stucture.

4.1 System Initialization:

Referring to Fig. 1, a tamper resistant electronic identification hardware unit is located in a safe, hard to replace area in the robot core electronic device. This device represents the robot identity to the outside world and should be tamper-proof and physically integrated in a core

mechanical unit of the robot. The initialization process could be accomplished by the following steps:

1. Manufacturer brands the unique robot serial number RSN on the robot as usual at the assigned label open to be read when needed. At the same time, manufacturer certifies the birth of the robot by inserting a secret key SDI0 in a write only memory within the tamper-resistant identity unit Fig. 4. The manufacturer is responsible for the uniqueness and secrecy of SDI0. He/she can use any secret mapping to generate SDI0 uniquely which needs not to be known to anybody else.
2. A true random generator is triggered once and only once to generate a secret mutated identity as described in [5] and [6] to generate a mutated secret device identity MSDI and eventually a secret hash function H'. Notice that MSDI and H' need not to be known to anybody. This operation is similar to a deliberate mutation (hyper mutation) generating a permanent DNA chain that is e-DNA for the particular robot.
3. A trusted authority TA records a part of the robot's e-DNA chain by securely challenging the identity module and storing a record of challenge-response pair list { C1, C2 … Cm }, { R1, R2 … Rm } and keeps it secret in TA's safe domain. If the trusted authority is not the same as the manufacturer, TA should store an electronic signature SDI1 correspondingly as the manufacturer did for SDI0 in step 1. The list { C1, C2 … Cm } is generated as follows:

$$Ci = H (SDI1, CHi) \qquad (1)$$

Where the set {CHi, CH2 … CHm} is selected by a secure random process and should be kept secret for later use.

The initialization is then completed and the robot is authenticated for that particular trusted authority. Making use of that identity is then possible in field operations. One possible "evolving identification" scenario is demonstrated in the following section.

4.2 Evolving Secured Identification Scenario:

To build robot own personal profile, a data logging store should trace selected real or mapped robot sensor and actors data. Fig. 5 shows a possible data logging scenario out of 4 robot sensors/actors data as vision, movement, Actor-stimulus or many other selected operational data. If a digest of these parameters is selected as Di and sent to a keyed hash function H using a secret key Ki, it would produce a response Si where

$$Si = H(Ki, Di) \qquad (2)$$

The hash response Si can cryptologically only be generated by somebody knowing Di and Ki. If i is a time index and the data logger is a write-once memory, then Si can be deployed as a hard to clone authentic signature as would be shown later.

A use-case scenario showing the benefits of the above evolving authentication can proceed as follows: Assume that the robot identity is to be remotely authenticated by TA after some operation time. Referring to Fig. 4 a "data logger" as a personal profile associated with the identity module can record sequentially the data packets Di's selected as those shown in Fig. 5. The data could even be kept anonymous towards TA. However TA should be enabled to challenge the device using an index i assigned to each personal profile packet. TA having the signature SDI1 can generate remotely and securely new evolved, time dependant challenge response pairs as follows (refer to Fig. 4):

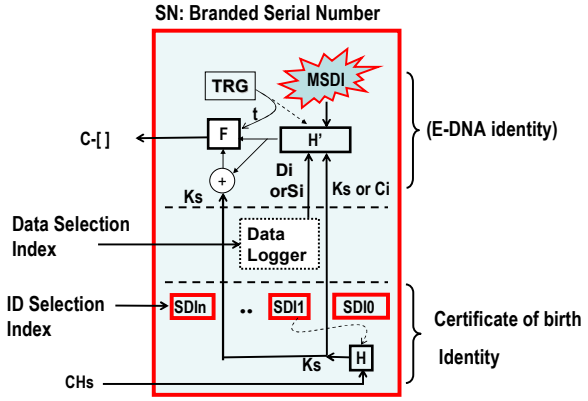

Figure 4. Hardware Core for a Living Identification Mechanism

1. A challenge from the initial list say CH2 is picked up by TA and sent to the robot device asking to prove its identity.
2. Device computes internally C2 = H(SDI1, CH2) and forwards it to H' to compute R2=H'(MSDI,C2) and encrypts R2|t as c-RES = $F(R2|t)_{K2}$ by the key K2=C2 XOR R2 (another nonlinear combination can be used for more security). Where t is a random fresh generated time stamp.
3. TA can decrypts c-RES as C2 and R2 are known to TA and gets R2|t. If R2 is correct, the robot identity is proved.
4. TA responds to the identity module by further actions using t as a fresh random key. If the identity module can decrypt reasonably, then TA is authentic towards the robot. This step can be saved in a further refinement if C2 is encrypted by itself and sent in step 1 and compared with the initially challenged C2. In this case a list of Ci set initially used has to be saved securely in the memory of the data logger.

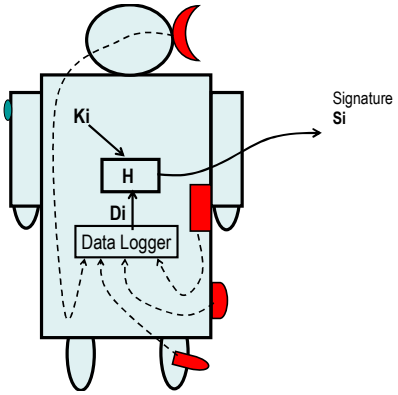

Figure 5. "Operation-Signature" and Robot Personal Profile

Now a new fresh C-R pairs using the following more complex hashing can be used

$$Ri = H' (MSDI, t, Ci, Di) \quad (3)$$

A dependency link between MSDI, SDI and personal profile is established. The new generated C-R pairs are a sort of living consistent identity proof for later time. The new C-R list at the TA site is dynamic and can from now on be used for further authentication using the same methodology shown above.

The index i represent a data logger packet index which can be selected by a secured random agreement between prover and verifier to avoid selective and repeatable proves and attacks. Other more sophisticated protocols for different applications and operation scenarios can be similarly developed. The particular properties of that technique are summarized as follows:

1. The system security is stable. As if somehow the identity module was successfully cloned, the system would fail and cloned pairs would be detected and stopped in future trials. The identification would divert due the personal profile changes after each transactions. At most very little false identifications can abuse the system, however in a traceable way.
2. The system can be securely resynchronized by repeating the 4 steps shown above with a non-used C-R pairs from TA's secret list.

Notice that The TA can not clone a robot identity and even the manufacturer would not be able to do it. It is assumed here that the manufacturer have not built backdoors in the hardware core. ***The resulting identity is somehow equivalent to a born baby where neither the parents nor the authentication authority can clone it without being detectable sooner or later.***

4.3 Mechatronic Security:

Linking the identity to the personal profile is a step towards associating acting and sensing units in a robot to the robot's identification scheme. The data profile for each actor or sensor as robot's sub-units can be seen as a part of its life history participating to define its identity. Hashing such data by using some keys can generate provable signatures linked to the robot unit's personal history as was shown in Fig. 5. Mechatronic security can be seen as the provable secured-relationship between a received stimulus and/or outgoing action from a robot mechanical or electronic unit. For example it could be necessary to know that a certain mechanical process was provably performed by a unit belonging to a certain robot to build a "chain of custody" for legal applications. If for a certain acting unit a signed history profile is recorded, then the recorded profile can be used in connection with the robot's mutated identity to show that a signature associated with a particular action is a proof that the unit associated with certain robot was the initiator of that action. The following mechatronic security functions can be given as examples for possible future requirements:

1. A robot should prove that he/she witnessed a certain event while doing its assigned job. Robot should offer a provable link between what he had seen and his own electromechanical activities.
2. A robot should prove having performed a certain mechanic effort.
3. A service or a mechanical action offered by a robot should not be deniable by the service receiver or vice versa.

Many other requirements could become necessary in realtion to existing robot tasks. A classification of such security requirements can be created through a joint collaboration within the interested research and/or user community.

VII. SECURITY THREATS

Detailed security analysis for the whole mechatronic robot environment seems to be difficult if not restricted to a certain application scenario. However basic security concerns of the proposed robot identification scenario can be discussed. The following security-threats and concerns are discussed similarly as in [6] adapted to the robots environment:

1. Robot initial personalization includes one-time non-reversible operations. A careful test strategy without backdoors should be considered. A collaborative scenario between trusted authority and manufacturer is necessary.
2. Due to the unpredictable and unknown random bit generation, the resulting values could be some bad ones and deliver information leakage or correlated

distribution of challenge-response pairs.

Possible Countermeasures: The system could increase the number of cycles used to minimize that risk in critical cases. However, the fact that neither information about H' nor MSDI makes attempts to crack the system hopeless for attackers. The attacker would most probably be only encouraged to work on an attack if his work would come up with a general cracking methodology with untraceable gain. This is quite un-expectable in such a varying environment and most probably leads to an early frustration as the identity trace is changing in a non-predictable manner. In addition to that, the probability of detecting successful attacks is inherently very high.

3. Due to possible temporary weakness resulting from the used unpredictable random sequences, a device may be easily cracked and cloned. Remedy: The structure is dynamic and even if a cloning becomes successful at any time point, at least the cloned or the original robot would fail to prove themselves at most after few transactions with a very high probability; both original robot and cloned robot would then be detected and tagged. The danger of fraud is stopped until the case is cleared and the cloned robot is identified by further investigations and can be made harmless. Therefore, the security of the whole system is still robust and stable.

VIII. Summary and Conclusions

The paper shows a scenario for integrating a clone-resistant identity in a robot system based on the recently developed e-DNA concept. A mechanism is proposed to link the robot identity to its interaction profile with the environment to keep the identity evolving in a traceable manner towards the trusted authority, The identity stays however untraceable for an outside observer. The mechanism exhibits highly secure and operational robot e-DNA identity marker which could approach the human DNA level of confidence. A sample evolving operative identification scenario is demonstrated. Mechatronic security linking robot identity to its mechanical and electronic actions is shown to be important for future robot tasks. Possible solution concepts for selected mechatronic security scenarios are also proposed.

References

[1] Gassend, B. Clarke, D. van Dijk, M. Devadas, S " Controlled physical random functions" Computer Security Applications Conference, 2002. Proceedings. 18th Annual, 2002,pp 149- 160

[2] G. Edward Suh*, Charles W. O'Donnell, Srinivas Devadas , " AEGIS: A single-chip secure processor". Information Security Technical Report (2005) 10,63e73

[3] P. Tuyls, RFID-Tags: Privacy and Security Issues, Philips Research

[4] John Butler; "Forensic DNA Typing, Second Edition: Biology, Technology, and Genetics of STR Markers" NIST-USA, ACADEMIC PRESS, 2005

[5] Adi, Wael; Soudan, Bassel; "Bio-Inspired Electronic-Mutation with genetic properties for Secured Identification", Bio-inspired, Learning, and Intelligent Systems for Security, 2007. BLISS 2007. pp.133 – 136

[6] Wael Adi, "Clone-Resistant DNA-Like Secured Dynamic Identity," BLISS 2008, Bio-inspired, Learning and Intelligent Systems for Security, 2008, pp. 148-153